What We Do

Transportation Security Administration

Haz Mat Safety & Security

The underground parking garage of the World Trade Center one day after the February 1993 explosion

Transportation Security Administration

"Aviation and Transportation Security Act" (Nov. 2001)

"(d) FUNCTIONS.—The TSA… shall be responsible for security in all modes of transportation including—
"(1) carrying out chapter 449, relating to civil aviation security, and related research and development activities; and
"(2) security responsibilities over other modes of transportation that are exercised by the Department of Transportation.

Transportation Security Administration

Administrator John Pistole's goal is for TSA to continue to grow as a risk-based, intelligence-driven counterterrorism agency dedicated to protecting our transportation systems.

TSA Surface Program Offices

Office of Security Policy & Industry Engagement (Surface Division)	Office of Security Operations (Surface Compliance)
• Regulatory & Voluntary Policy Development • Analysis • Stakeholder Support and Coordination	• Regulatory Compliance • Voluntary Assessments • Operational Support

Transportation
Security
Administration

OSPIE Mission Statement

OSPIE develops security policies and plans designed to reduce the risk of catastrophic terrorist attacks.

We do that by:

- Focusing on nationally significant risks

- Building strategic Industry partnerships

- Producing risk-based policies and plans with measurable outcomes

Highway & Motor Carrier Landscape

- Trucking –
  - 700K+ companies, 8.8M trucks, 70K HAZMAT
- Motorcoach –
  - 4500 companies, 30K buses, 750M passengers
- School Bus –
  - 500K school buses, 25M students
- HWY Infrastructure –
  - 4.25M miles of highways, interstates, roads
  - 604K bridges and 350 tunnels

- Truck vs Bridge/Tunnel

# Surface Division Four Security Pillars

- **Assessments & Information Sharing**
  - Baseline Assessment for Security Enhancement (BASE)
  - Industry Concerns
  - Data Collection
  - Structural and Modal Assessments
- **Security Plans (Voluntary and Regulatory)**
  - Guidance
  - Templates
- **Training**
  - Counterterrorism (Guides)
  - Domain Awareness (SSSS/First Observer™)
- **Exercises (I-STEP/EXIS)**
  - Intelligence & Information Sharing Network
  - Lessons Learned

Assessing Risk (R=TVC)

THREAT – Thru Coordination with Intelligence Community / LE

- AQAP Inspire Magazine (HSIN)

  - "Strategy of 1000 cuts"

  - "Bleed the enemy to death"
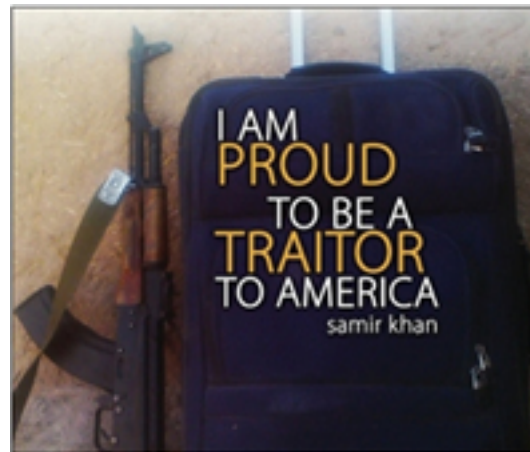
Samir Khan's article in the second issue of *Inspire*

Front cover of the November 2010 issue of *Inspire*

Assess Risk (R=TVC) Cont…

VULNERABILITIES – Identification of Security Gaps

CONSEQUENCES – Direct: Deaths, Injuries, Damages

Indirect: Economic, Psychological, impact at Local, Regional or National level

Historical Perspective – Long Term

February 26, 1993
World Trade Center
New York City, NY

Ramzi Yousef, Mahmud Abouhalima, Mohammad Salameh, Nidal A. Ayyad, Abdul Rahman Yasin, Ahmad Ajaj, and Khaled Shaikh Mohammed

A rental truck loaded with 1,500 lbs of urea nitrate-hydrogen gas was detonated in the parking garage of the North Tower in an effort to bring down both towers. 6 killed, 1,042 inured.
(7 conspirators convicted)

9/11 Attacks

September 23, 2009
Paul Findley Federal Bldg
Springfield, IL

Michael Finton, aka Talib Islam

Michael C. Finton, 29, who also went by the name Talib Islam, was arrested in Springfield IL, after federal officials said he attempted to set off explosives in a van outside a federal courthouse in the state capital.
(Trial Pending)

May 1, 2010
Times Square
New York City, NY

Faisal Shahzad

Shahzad parked a Nissan Pathfinder loaded with a homemade bomb in Times Square, activated a timer, and fled. The bomb failed to detonate.
"Brace yourselves, because the war with Muslims has just begun" …. "Consider me the first droplet of the blood that will follow."
(Oct, 2010 - Sentenced to Life without Parole)

1993   1994   1995   1996   2001   2008   2009   2010   2011

April 19, 1995
Alfred P. Murrah Federal Building
Oklahoma City, OK

Timothy McVeigh

McVeigh detonated a rental truck loaded with 7,000 lbs of ANFO and nitromethane in front of the federal building in Oklahoma City. 168 killed, 450 injured.
(June 11, 2001 – McVeigh was executed)

September 24, 2009
Fountain Place
Dallas, TX

Hosam Husein Smadi

Smadi acknowledged leaving what he thought was a truck bomb in a garage beneath the 60-story Fountain Place building. Smadi said he parked the truck, activated a timer connected to the decoy provided by undercover FBI agents, then rode away to watch the explosion.
(Oct, 2010 - Sentenced to 24 yrs Fed Prison)

November 26, 2010
Christmas Tree Lighting Ceremony
Portland, OR

Mohamed Osman Mohamud

A 19-year old Somali-born teenager attempted to blow up a van full of explosives at a crowded Christmas tree lighting ceremony in downtown Portland. Mohamud drove to downtown Portland in a white van that carried six 55-gallon drums with detonation cords and plastic caps.

Two Companies Stopped a Terror Suspect - 2/24/2011

Employees from Conway Freight in Ann Arbor, Michigan and Carolina Biological Supply in Burlington N.C. both called police to report suspicious purchasing activity. Security training made them suspicious.

Suspect attempted to purchase and ship chemicals and equipment to Texas needed to make improvised explosive devices (IEDs).

POTENTIAL VBIED

CAROLINA®
World-Class Support for Science & Math

Domestic Trucking Incidents 2012

(U//FOUO) Truck

- Methods
    - IED
    - CYBER

(U) December 10, 2012, Oklahoma City, Oklahoma *(IED Devices)-* Police found and disabled two pipe bombs at an Oklahoma City trucking company December 10. The Oklahoma City Police Department bomb squad said the two bombs found at the Majerus Trucking Co. were "viable and working." Officers said the bombs were found under a truck at the facility. *Source:* http://www.koco.com/

(U) Actor Probably Targeting Trucking Business Finance Portals to Test Profitability On Dec. 6, 2012, a Citadel campaign targeting only finance management portals used by trucking businesses was observed. On Dec. 7, 2012, another Citadel campaign was observed that targeted the same trucking finance management portals as well as several banks and other major financial institutions often targeted by cybercrime actors. Since the same C&C and encryption key was used in the Dec. 6 and 7 campaigns, the same actor is almost certainly responsible. The addition of more traditional targets provides some indication that targeting just trucking businesses was not as profitable as the actor had hoped. *Source: trusted 3rd party*

Domestic Trucking Incident 2013

(U//FOUO) Truck

- Methods
    - IED (Threat Only)

(U) September 11, 2013, Hampton, Virginia (Terrorist Bomb Threat) - At 0930 hours on September 11 Norfolk SCCO reported telephonically that at 0800 hours, Virginia State Police (VSP) received a telephonic bomb threat from an unidentified individual with a middle-eastern accent who stated, "between 0900 hours and 1200 hours, a truck loaded with a bomb would be driving through the Hampton Roads Bridge Tunnel in Hampton, VA. VSP requested a US Coast Guard Maritime Security Response Team K-9 Unit and a Bureau of Field Operations K-9 Unit. VA. VSP Fusion Center, Bureau of Criminal Investigation, Criminal Investigation Department and JTTF were notified. LEOs are attempting to trace the call. Initial information is that the tunnel remains open and LEOs are searching all trucks. At 1030 hours, TSOC notified OSPIE Highway and Motor Carrier. No further information provided at this time.

Overseas Truck Attacks 2013

(U//FOUO) Trucking Attacks – 68 Attacks
- Methods
    - VBIED – 18
    - Arson – 13
    - Active Shooter – 12
    - Assassination – 8
    - Stand-off – 6
    - Suicide – 5
    - Hijacking – 3
    - IED – 3

Understanding the Terrorist Planning Cycle

- **Broad Target Selection**

- *General Indicators* - Expressing interest in and researching of potential targets

- **Training**

- *General Indicators* - Obtaining, or expressing interest in obtaining, and using weapons, explosives, and bomb-making manuals for use in violent actions

- **Intelligence Gathering and Surveillance**

- *General Indicators* - Taking action to collect information on a specific Target

- **Specific Target Selection**

- *General Indicators* - Expressing desire to attack a specific target

- **Pre-Attack Surveillance and Planning**

- *General Indicators* - Attempts to gain access into secured areas without reason to enter

Terrorist Planning Cycle Cont…

- *General Indicators -* <u>Seeks information of exposed areas or equipment. Questions what would shut down or damage the business or equipment</u>

- **Attack Rehearsal**

- *General Indicators – <u>Use of rental, stolen or other vehicles for dry runs</u>*

- *General Indicators – <u>Deploying suspicious items to test response by security personnel</u>*

- **Actions on the Objective**

- *General Indicators -* <u>Vandalism involving damage to security cameras or other security devices</u>

- **Escape and evasion**

- *General Indicators – <u>Pre-staged vehicles or equipment</u>*

- *General Indicators – <u>Pre-purchased travel arrangements or documented transportation schedules</u>*

Eight Signs of Terrorism

1. **Surveillance**

2. **Elicitation**

3. **Tests of Security**

4. **Funding**

5. **Supply**

6. **Impersonation**

7. **Rehearsal**

8. **Deployment**

Attack Methods - Trucking

- **Vehicle Borne Improvised Explosive Device (VBIED)**

- Improvised Explosive Device (IED)

- Improvised Incendiary Device (IID)

- Active Shooter (Mumbai/Ft Hood)

- Insider (behavior recognition)

- Theft

- Stand Off

- Hijackings

- Cyber
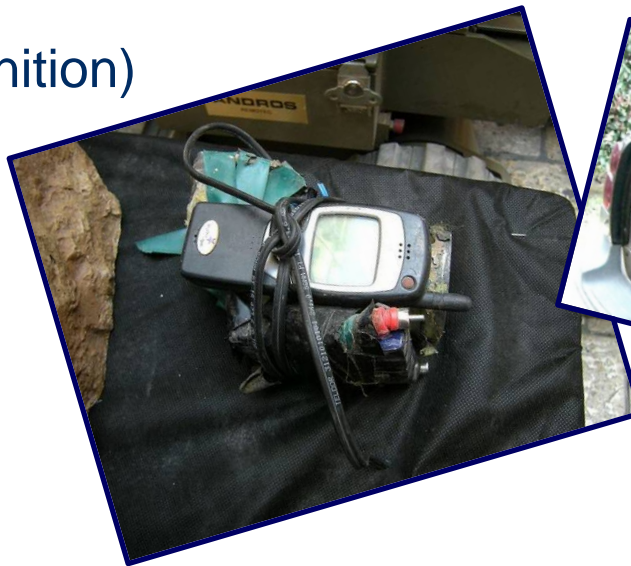
Indicators

- **Vehicle Borne Improvised Explosive Device (VBIED)**
  - Vehicle riding low in the rear (sagging vehicle)
  - Illegally parked or near authorized vehicle entrances or crowded access points
  - Covered or tinted windows
  - Large containers on seats or cargo area: bags, boxes, barrels, tanks
  - License plates removed or altered
  - Odor of gasoline, propane, acids, or chemicals
  - Acrid smoke – indicates possible lit fuse
  - Visible wires, switches, batteries, or antennae inside or on vehicle
  - Cargo concealed with tarp or blanket

ILLEGALLY PARKED VEHICLES WILL BE TOWED AT VEHICLE OWNER'S EXPENSE

What You Can Do to Enhance Security

- Develop a Strong Security Plan
- Participate in *Highway BASE* Program

OR

- Self Assess Your Security Using *T-START*

Security Planning

What Does a Good Security Plan Look Like?

1. Security Statement and Markings (49CFR1520)

2. Company Information, Goals and Objectives

3. Risk Assessment R = TVC

   ➢ Threat – what are the most likely attack methods?
   ➢ Vulnerability – what type of attacks are you susceptible to?
   ➢ Consequence – what is the direct (i.e. deaths, injuries, damage) and indirect (i.e. economical, psychological, local, regional, national levels) impact?

What Does a Security Plan Look Like?

4. Management / Accountability

   ➤   Designated Security Coordinator

   ➤   Emergency Response

   ➤   Security Protocols (SOPs)

   ➤   Continuity of Operations (COOP)

   ➤   Communications Plan

   ➤   Business/Security Critical Information

   ➤   Awareness of Industry Best Practices

   ➤   Inventory Control

What Does a Security Plan Look Like Cont…?

5. Personnel Security
    ➢ Valid CDL & Endorsements
    ➢ Background Checks
    ➢ Training Plan (security awareness)
    ➢ Security Exercises and Drills
6. Facility Security
    ➢ Access Control
    ➢ Physical Security
    ➢ Cyber Security
7. Vehicle Security
    ➢ Vehicle Security Program

What Does a Security Plan Look Like Cont…?

7. Vehicle Security Cont…
   - ➢ Cargo / Passenger Security Program
   - ➢ High Alert Level Protocols
   - ➢ Security Inspection Policy and Procedures
   - ➢ Reporting Suspicious Activities and Procedures
   - ➢ Chain of Custody / Scheduled Service or Shipment
   - ➢ Preplanning Emergency Routes
8. Revisions Log
   - ➢ Name, Date, Change made
9. Non-disclosure Agreement
10. Appendices (templates/forms/checklists)

What is the Highway BASE?

__B__aseline __A__ssessment for __S__ecurity __E__nhancement

- Free and ***voluntary*** on-site security assessment

- A review of your security program with options to consider toward reducing risk

- Results in a written report with multiple components

- Developed by TSA with input from industry

Transportation
Security
Administration

BASE Done by TSA Surface Field Offices
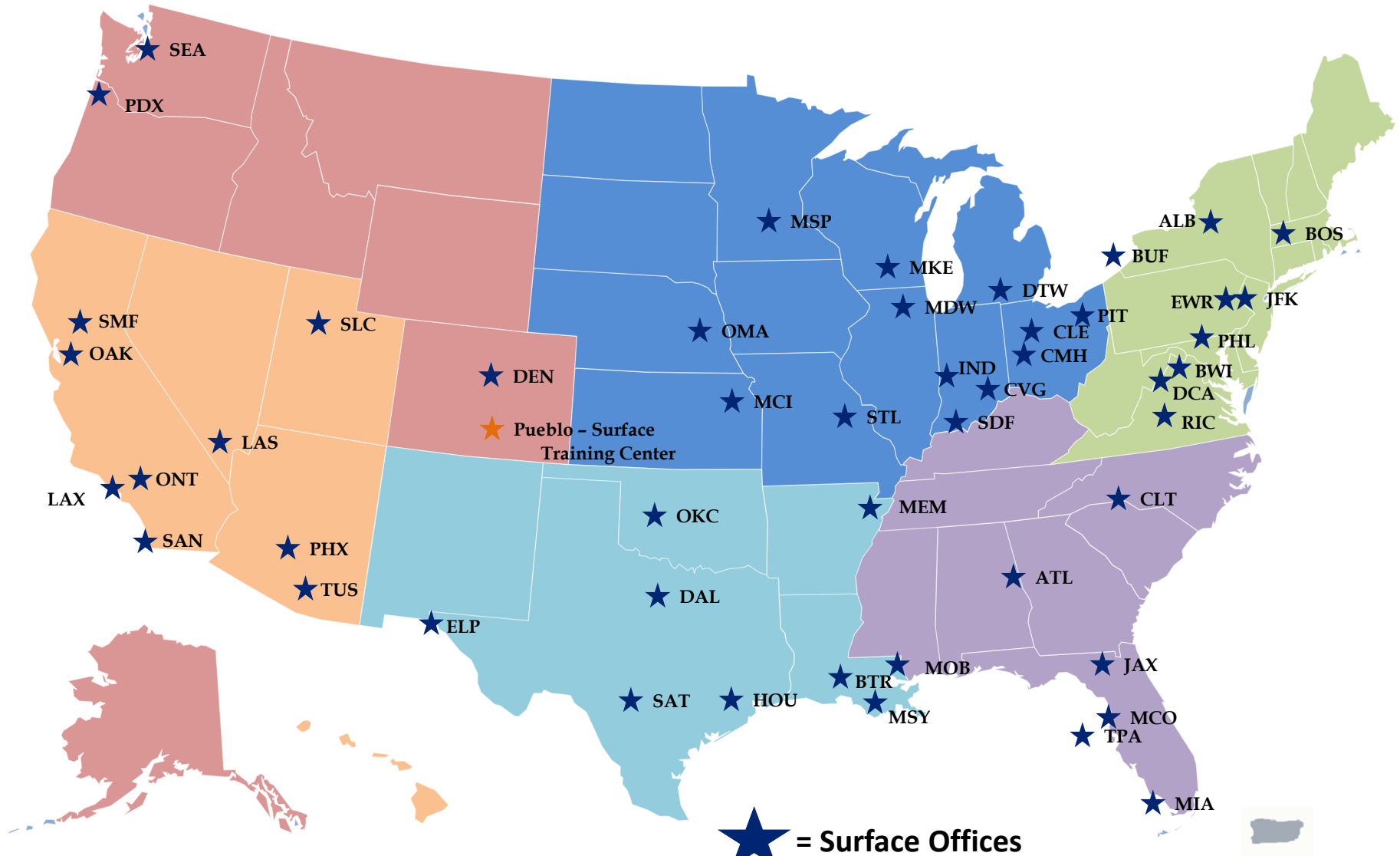
★ = Surface Offices

★ = Training Center

Transportation
Security
Administration

Misconceptions

The BASE is NOT:

- – ***Not*** a compliance/regulatory inspection
- – ***Not*** used to enforce or supplement compliance/regulatory inspections
- – ***Not*** a test
- – ***Not*** legally binding
- – ***Not*** used by other Federal Agencies
- – ***Not*** a "screening" initiative

Transportation
Security
Administration

What Does the BASE Cover?

Four General Areas

- ***Management and Accountability***
- ***Personnel Security***
- ***Vehicle Security***
- ***Facility Security***

4 General Areas divided into twenty (20) SAIs

- Security Action Items

20 SAIs Divided into

- 99 specific security line items (questions)
- Each Scored 0-4 by you and inspector

Transportation
Security
Administration

What Highway BASE Provides

A narrative "Executive Summary" Report

A "Scorecard" with two scores:
- Overall Security Score
- Critical Elements Score

Transportation
Security
Administration

BASE Sample Scorecard

SAI #	SECURITY ACTION ITEM (SAI'S) DESCRIPTION	Performance
1	Have a Designated Security Coordinator	68%
2	Conduct a Thorough Risk Assessment	75%
3	Develop a Security Plan (Security Specific Protocols)	80%
4	Plan for Continuity of Operations	75%
5	Develop a Communications Plan	88%
6	Safeguard Business and Security Critical Information	83%
7	Be Aware of Industry Security Best Practices.	62%
8	Conduct Licensing & Background Checks for Drivers / Employees / Contractors	83%
9	Develop and Follow Security Training Plan(s)	83%
10	Participates in Security Exercises & Drills	75%
11	Maintain Facility Access Control	55%
12	Implement Strong Physical Security at all Locations	84%
13	Enhance Internal and External Cyber Security	79%
14	Develop a Robust Vehicle Security Program	88%
15	Develop a Solid Cargo/Passenger Security Program.	55%
16	Plan for High Alert Level Contingencies	61%
17	Conduct Regular Security Inspections	57%
18	Have Procedures for Reporting Suspicious Activities	81%
19	Ensure Chain of Custody & Shipment/ Service Verification	62%
20	Pre-plan Emergency Travel Routes.	100%
	Overall Performance Score:	75%
	Critical Elements Score:	77%

Transportation
Security
Administration

Post Review BASE Provides

Full Report delivered

- Executive Summary (narrative)
  - Strengths
  - Weaknesses
  - Options for Consideration
- Security Scores

Follow-up from TSA in 1-3 years

Follow-up (again) is voluntary

Transportation
Security
Administration

Highway "T-START"

Transportation Security Template and Assessment Review Toolkit

3 Modules

❖ Security Management Overview and Understanding Risk

❖ How to Conduct a Vulnerability Assessment (with Vulnerability Self-Assessment Tool) and Security Options to Consider

❖ Security Plan Guide & **Template**

Transportation Security Template and Assessment Review Toolkit (T-START)

Security Sensitive Information

Transportation Security Administration
Office of Security Policy & Industry Engagement
Surface Division
Highway & Motor Carrier Branch

T-START
Transportation Security Template and Assessment Review Toolkit

A Security Awareness Guide

October 2013

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

1

T-START

Transportation Security Template and Assessment Review Toolkit (T-START)

- Designed for Non-BASE Participating Companies
  - ✓ Smaller Companies
  - ✓ Security may be new or still developing
  - ✓ Companies not visited by TSA (Risk-based)
  - ✓ HazMat Companies

Security Awareness Guide – Module #1

Any Security Items Not Up To Par Produce

"Mitigation Priorities" – list of corrective actions that should be addressed, and in what order

- **High Priority** *(Immediate Corrective Actions May be Warranted)*

- **Medium Priority** *(Prompt Corrective Actions Recommended)*

- **Low Priority** *(Corrective Action Recommended at earliest convenience)*

Transportation
Security
Administration

T-START

- Lacks the Objectivity of BASE
- Provides no Scorecard
- Has no Executive Summary
- Has no TSA post-review feedback
- You do the work – not TSA

It has value to the 1000's who will not participate in BASE
BUTT
Is not a substitution for BASE

Transportation
Security
Administration

Summary

BASE & T-START

- Are <u>voluntary,</u> non-regulatory security tools

- Are <u>free</u> security assessment tools to improve security

- Can be <u>tailored</u> to the needs of the stakeholder

- Are a <u>stepping-stone</u> for continued collaboration

- Are a <u>resource</u> available through your local TSA Surface Office or HQ – Surface Division

Transportation
Security
Administration

The Way Forward

- Improve the Information Sharing Network
  - Highway and Surface Information Sharing and Analysis Center (ISAC)
  - State Fusion Centers
  - Joint Terrorism Task Force (JTTF)
  - Transportation Security Operation Center (TSOC)
  - Private and Public Stakeholders
  - Homeland Security Information Network (HSIN)
  - National Terrorism Advisory System (NTAS)

- Intelligence and Security Information Products
  - Tactics, Techniques and Procedures
  - Transportation Intelligence Note
  - Unclassified Briefings
  - Risk Mitigation Analysis
  - Classified Material

- Continue to coordinate & collaborate with private and public stakeholders
  - Identify security gaps and recommend actions to close gaps
  - Develop tools and resources to enhance the overall security posture
  - Develop and provide guidance on preventing and protecting critical assets from terrorist attacks

Cyber Security Best Practices

➢ Ensure all IT systems require unique login credentials for all users (no shared user accounts and no blank passwords)

➢ Do not allow personal thumb drives on corporate networks or computers

➢ Beware of the insider threat:

  ➢ Immediately remove account access for employees who leave the organization

  ➢ Do not become overly reliant on a single employee to manage critical systems

  ➢ Create a system for employees to safely report suspicious behavior

➢ Use strong passwords; at least 8 characters (numbers, letters, and special characters)

➢ Limit remote access to systems and track access log files

DHS Cyber Resources

- **Cyber Security Evaluation Tool (CSET)**
  - Free tool available to organizations interested in assessing and improving their cyber security posture
  - http://ics-cert.us-cert.gov/satool.html

- **United States Computer Emergency Readiness Team (US-CERT)**
  - Provides cyber incident response for federal government
  - Provides cyber alerts and security tips (available to the public)
  - www.us-cert.gov

- **TSA Cyber Security Awareness and Outreach**
  - Provides a link between transportation industry and federal government
  - Email us at : cybersecurity@tsa.dhs.gov

https://cs.hsin.gov/default.aspx

Live Search

File   Edit   View   Favorites   Tools   Help

HSIN CS Portal - CS ...   x   TSA iShare

Page ▼   Tools ▼

HSIN-CS

My Site   Help

| CS Home | Sectors | DHS Document Highlights | Daily OSIR | Cyber Information | User Information | Connect! |

CS Home

All sources

Pandemic Flu Information | NISAC Library | BP Oil Spill Response | 2010 Hurricane Season | Hurricane Earl |

Today's date is Thursday, October 14, 2010

DHS Document Highlights

All portal users

- (U) Inspire Magazine 10122010.pdf
- (UFOUO) HSN - Mexico Nuevo Leons New Security Plan Unlikely to Quell Violence 10042010.pdf
- Current Situation Report - Chemical Plant Fire Sheffield, IL - 10 Oct 10 (Final)
- Current Situation Report - Explosion at Clarion Inn Hotel - San Pedro CA - 10 Oct 10 (Final)
- NICC Spot Report Explosion, Clarion Hotel San Pedro, CA - 10 Oct 10
- NICC Spot Report Euclid Chemical Plant Sheffield, IL - 09 Oct 10

Recent DHS I&A Products

Name

(U) Inspire Magazine 10122010.pdf
(UFOUO) HSN - Mexico Nuevo Leon's New Security Plan Unlikely to Quell Trafficker Violence 10042010.pdf
(UFOUO) JIB - Al-Qaida Threat to Europe 10032010.pdf
(UFOUO) HSN - Violent Extremists Suggest Tactics to Defeat Postal Sector Procedures 09232010.pdf
(UFOUO) DHS I-A Analytic Product Line SEP10.pdf

Recent HITRAC Products

Name

20100902 2051 IIA Hurricane Earl External - FINAL.pdf
IP Note_Attack Russian Power Station 081210.pdf
IP Note_Food and Agriculture Vulnerability 081210.pdf
Rapid Analysis Midwest Flooding Impacts of Mississippi River Closure_2008.ppt
Foundational Methodology to Support Infrastructure Decision Analysis - Initial Development and Test Case_2010.pdf

Toolbox

Tools

Contact Us

HSIN-CS All Sector Document Library

Links

CIKR Open Source News Feeds

National Level Reporting

Subscribe to receive
"New Posting Notifications"
from the National Infrastructure
Coordinating Center (NICC)

Quicklinks to Recurring Reports

- NICC Daily Pulse
- DHS Daily Open Source Infrastructure Report
- DHS Monthly Sector Open Source Digests
- DHS Monthly Open Source Cyber Digest
- DHS-OSE Daily Open Source Reports

HSIN-CS Communities

Sectors

CIKR Education, Training and Outreach
CIPAC - Trade Association Site
Fusion Centers Landing Page
Healthcare and Public Health
Highway and Motor Carrier
HITRAC
Industrial Control Systems Joint Working Group (ICSJWG)
Infrastructure Protection (IP) Data Exchange Partnership
TRIPwire Community Gateway
TSA-OI

DHS Document Highlights
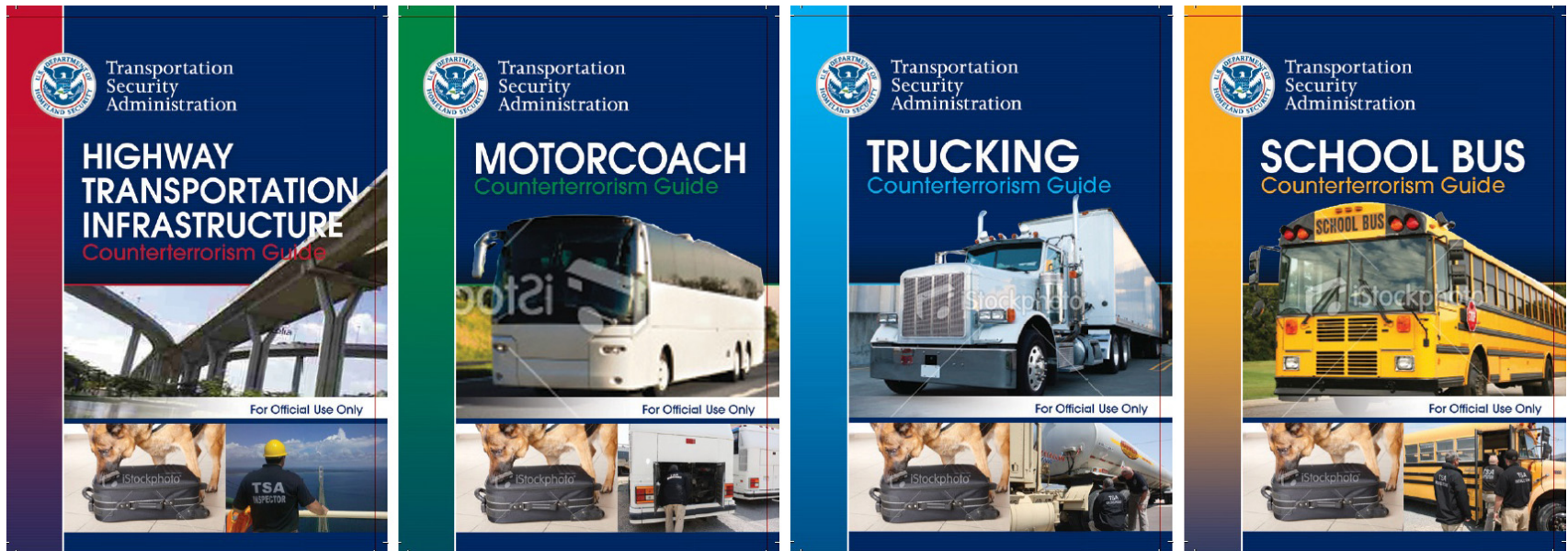
Daily OSIR

Cyber Information

User Information

Start   Inbox -...   SAI's   Micros...   HSIN...   Search Desktop   10:51 AM

Counterterrorism Guides

Available at website: www.TSA.gov/highway
Or email : highwaysecurity@dhs.gov

Security Action Item Training CD/DVD

First Observer™ Training (under re-development)

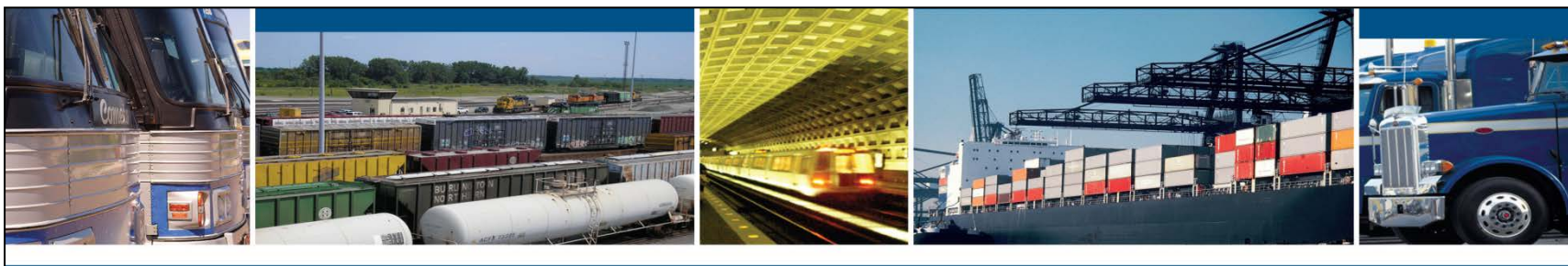**14 Different Training Modules- Available On Line**

www.TSA.gov/FirstObserver

TSA Trucking Exercises

Intermodal Security Training Exercise Program (I-STEP)

Trucking Exercise Set for September 4, 2014
Los Angeles, CA

Others being discussed for 2015

**Intermodal Security Training
Exercise Program (I-STEP)**

Transportation
Security
Administration

Transportation
Security
Administration

William "Bill" Arrington
Industry Engagement Branch Manager
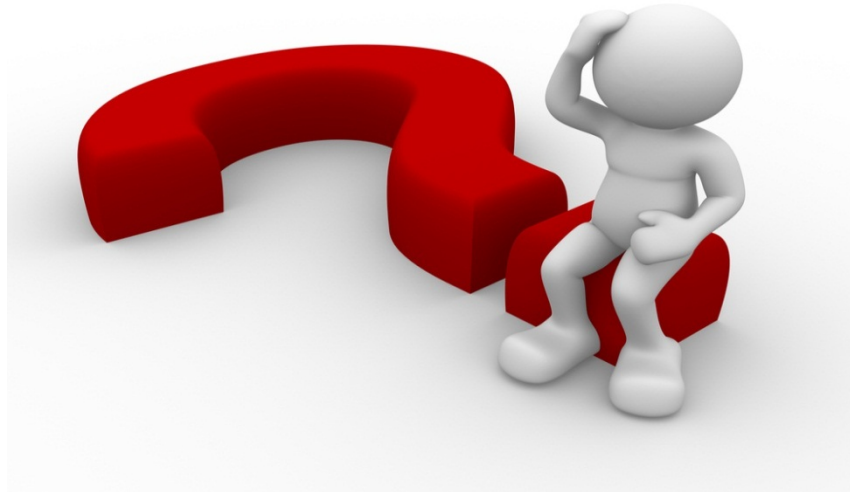William.arrington@dhs.gov
571-227-2436

David Cooper
Highway Sector Modal Manager
Industry Engagement Branch
David.cooper1@dhs.gov
571-227-2609

Ken Ward
Industry Engagement Support Section
Kenneth.ward@dhs.gov
571-227-2621

Transportation
Security
Administration

TSA Highway E-mail:
Highwaysecurity@dhs.gov

TSA Highway Website
www.tsa.gov/highway
(Under Re-construction)

Transportation
Security
Administration

Transportation
Security
Administration